Technical Cybersecurity

Malvertising

Online Advertising

The players

- **Advertiser**: Someone who needs some advertising
- **Advertising Agency**: Hired by the advertiser, creates the content and registers with the Ad Network
- **Ad Network**: Facilitates the sale and display of advertising across publishers and advertisers
- **Publisher**: Publishes ads, has ad space on web properties called *Advertising Inventory*

Online Advertising

The process

- The advertiser has already worked with the advertising agency, who has developed a campaign and ads that need to be published.

1. Advertising agency registers with an ad network (e.g. Doubleclick) with the types of ads they'd like to run and the types of customers they're interested in. This includes bids for advertising space.
2. A publisher affiliated with the ad network has a request come into a web page. That page has advertising associated with it. Prior to displaying the page, the publisher registers the request with the network.
3. The ad network publishes the demographic data of the user requesting the web page and requests bids for advertising.
4. Interested agencies bid on the ad space, and the highest bid wins. That bid pays the second-highest amount, with some small markup (usually).
5. That ad is delivered to the publisher and displayed to the user.

What *are* online ads?

Small web pages

- Online ads are small web pages that are able to display in very specific ways.
  - Banner ads
  - Popup/popunder ads (much more rare today)
  - Skyscraper (or sidebar) ads
  - In-text ads
  - Pushdowns
  - …and much more :-((see: http://showcase.sizmek.com/formats/)

An Example

An Adobe ad from Slashdot

What's in the Ad?

IFRAME

- We have multiple iFrames
  - IFrames are essentially frames in HTML that allow you to render an entire HTML page. They are powerful and frequently used in browser-based attacks.

JAVASCRIPT & HTML

- Javascript provides dynamic behavior in web pages
  - This includes asynchronous processing (webworkers, timers) and extensive network communication capabilities (websockets, XMLHttpRequests)

Perfect for Access

Malicious ads

- They can get access to the browser and…
  - …break out
  - …scan
  - …ask users to install
  - …just hang around and do whatever
- May not have that much time though

And you can profile your targets!

How to get into ad networks?

Register ads for fake companies

- Just register malicious ads directly (not so common today)

Register ads for real companies

- Then change the ads

Submit ads for trojans

- Amazing what people will click on

Why not create your own network?

Protect yourself!

Don't click on internet ads

- Usually malvertising requires a manual trigger

Install an ad blocker

- Ad blocker authors and advertising platforms are in a battle for your eyes

Install a Pi-Hole

- Protect your entire network!

Exploit kits!